JC Res'd PCT/PTO 1 1 FEB 2002

E6369-01EX

INFORMATION UNDER 37 CFR 1.56(a) (For Initial Filing)

The following references are submitted as information to comply with the duty of disclosure under 37 CFR 1.56(a):

ſ		Disclosed	d in the		Сору	Translation			
	References	specifica Yes	No	Enc.	Follow	Please obtain	Enc.	Not avail- able	
,	1. Efficient elliptic curve exponentiation using mixed coordinates, Advances in Cryptology Proceedings of ASIACRYPT'98, LNCS 1514, Springer-Verlag, (1998) pp.51-65	0		0				able	
	2. P.L.Montgomery, Speeding the Pollard and Elliptic Curve Methods of Factorization, Math. Comp. 48 (1987), pp.243-264	. 0		0					
1	3. Fast Multiplication on Elliptic Curves over GF(2 ^m) without Precomputation, Cryptographics Hardware and Embedded Systems: Proceedings of CHES'99, LNCS 1717, Springer-Verlag, (1999) PP.316-327	· O		0					
1	4. Elliptic Curves with the Montgomery-Form and Their Cryptographic Applications, Public Key Cryptography, LNCS 1751 (2000) PP.238-257	0		0					
	5.								
	6.								

Examiner:

DATE CONSIDERED

6/7/6

FORM Comme	PTO	-144	9 U	.S. D	eparl	ment	of	Ē\	6,29	ATT	. DOCKET NO.		SERIAL NO.				
Comme						/() `	500	41178X00	10/049,264							
				ON D T BY							ICANT KEYA	_					
		(Use s	several	T BY	if nece	essery	Arn So	_ «.	NEG.		IG DATE tember 30, 20	02	GROUP				
						U	.S. P	ATE	NT	DOC	UMENTS						
EXAMINER						·							T		FILING	DATE	
INITIAL	 	DOCUMENT NUMBER				 			ATE	E NAME		CLASS SUBCLAS		IF APPROPRIATE			
	 		-			\vdash	-		┾┈				+	· · ·			
			ļ	-		 	├	 	 				-		ļ		
	<u> </u>						<u> </u>	 	-				_				
	<u> </u>		ļ			_	_		<u> </u>								
				<u> </u>		ļ	ļ						_				
			<u> </u>			ļ	<u> </u>	<u> </u>	_								
				<u> </u>	<u> </u>		<u> </u>										
						<u> </u>											
							<u></u>										
FOREIC	SN P	ATE	NT [DOC	JME	NTS					•	· · · · · · · · · · · · · · · · · · ·					
			MENT N						0	ATE	COUNTRY	RY CLAS	S SUBCLASS	SUBCLASS	ABSTRACT		
MA	<u> </u>				,									YES	NO		
<i>\\/</i> .		9	9	4	9	3	8	6	9/9	9	РСТ		_			<u> </u>	
1									<u> </u>								
							<u>l</u>										
OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)														·			
						<u></u>		, •		, _ = .							
	П											······································			, = -		
	\Box																
EXAMINE	I R	DATE CONSIDERED 6/7/6															
EXAMINER: Initial if citation is considered, draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.																	

(Form PTO-1449 [6-4])